Campanha de Phishing

Citeforma | CET 8493 | UFCD 9195 Enquadramento operacional de cibersegurança | Formador: João Almeida

Hugo Miguel Félix Bugalho | João Rodrigo Mota da Costa | João Miguel Oliveira da Costa

Introdução

Neste documento , iremos documentar o planeamonto de um site de phising, explicando quem será a população alvo, o conteúdo do email, e como iria ser o site. Este trabalho foi feito de acordo com as instruções dadas pelo formador João Almeida.

Desenvolvimento do projecto

População alvo

O nosso grupo alvo serão princípalmente adultos, particularmente entre as idades de 35 e 65 anos porque são o grupo mais provável de usar websites de homebanking num browser. Nós decidimo-nos focar nesta faixa etária, pois pessoas abaixo desta idade estão mais habituadas e conhecem melhor o conceito de uma app do que de um website; E regra geral, pessoas acima dos 65 não têm conhecimento tecnológico suficiente para utilizar um computador, quanto mais uma aplicação de homebanking. Caso tenham e utilizem esses serviços, fazem parte do público alvo.

O que oferecemos

Nos nossos emails, nos oferecemos "ajuda" para uma situação das quais as vitimas não têm controlo e instaurar um sentimento de urgência para forçar a vitima a abrir a página e inserir as suas credenciais. Se estas levarem a um erro ainda mais "assustador", pode causar uma situação ainda mais interessante em que a vitima contacta o balcão e o próprio banco pode entrar em pânico ou então ter de ser os mensageiros a explicar ao cliente que foram vitimas de uma "burla" (aka um ataque de phishing).

Conteudo do email

Seriam enviados E-mails de atualização de conta, explicando que a conta tinha sido acedida de um país diferente, por isso poderia estar comprometida. Estaria um link associado para o site falso. No link enviado por mail, os utilizadores são solicitados a inserir as suas informações confidenciais, como nome de usuário, senha, número de conta bancária, PIN ou outros dados relevantes, para verificar identidade e poder fazer a troca de password.

Descrição do site

O site iria ter um url parecido ao original, para não ser suspeito; ia manter o design e logótipos o mais semelhante ao site original possível; e os pedidos de informação seriam justificados, não simplesmente aparecer um pop-up a pedir os dados. ste site, a vítima poderia carregar em vários links, que redirecionariam para páginas idênticas à do site oficial (homepage, espaço cliente, contactos, etc). Mostramos abaixo alguns exemplos de sites que gostariamos de ter replicado.



Conclusão

Com estre trabalho, foi possível compreender como utilizar engenharia social e de técnicas fraudulentas para obter informações pessoais e financeiras das vítimas. Ao explorar ataques por sites falsos e e-mails fraudulentos, torna-se evidente a importância da conscientização e da adoção de medidas de segurança adequadas para nos protegermos contra tais ameaças. É essencial que as pessoas estejam atentas aos sinais de possíveis ataques e saibam como identificar e relatar atividades suspeitas.